The 23rd Annual International Conference on Information Security and Cryptology

ICISC 2020

December 2 (Wed) ~ December 4 (Fri), 2020 | Virtual Conference

Hosted by

Korea Institute of Information Security and Cryptology (KIISC)

National Security Research Institute (NSR)

An Efficient Authenticated Key Exchange from Random Self-Reducibility on CSIDH

Tomoki Kawashima [†], Katsuyuki Takashima [‡],

Yusuke Aikawa [‡], and Tsuyoshi Takagi [†]

[†] *University of Tokyo, Japan*

[‡] *Mitsubishi Electric Corporation, Japan*

Table of Contents

Table of Contents

Post-Quantum Cryptography & AKE

- Current cryptosystems (Diffie-Hellman, RSA, etc.) will be broken by Shor's algorithm [Sho97] with quantum computers.
- CSIDH [CLM+18]
  - Post-Quantum Key Exchange
  - Similar structure to DH
- DH and CSIDH are vulnerable to the man-in-the-middle attack.
  - We need Authenticated Key Exchange (AKE).

[Sho97] P.W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Computing, 26(5)*

[CLM+18] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. CSIDH: An Effic-ient Post-Quantum Commutative Group Action. In *ASIACRYPT 2018*

Tightness

- Π: Protocol, P: hard problem
- In the security proof, we have $\mathrm{Adv}_{\Pi}^{\mathcal{A}}(\lambda) \leq L(\lambda) \cdot \mathrm{Adv}_{P}^{\mathcal{B}}(\lambda)$.
  - $L(\lambda)$ is called security loss.
  - If security loss is large, larger parameters are used, thus inefficient.
- Many post-quantum AKEs have been proposed, but security losses are large.

Can we construct a post-quantum AKE
with small security loss?

Contribution

1. We prove that the computational problem of CSIDH and the gap problem of CSIDH are random self-reducible.
   - Random self-reducibility of a hard problem is useful to achieve tightness of protocols
   - Gap problem is a computational problem given access to the corresponding decision oracle.
   - Gap problem is very useful for AKE's security proof.

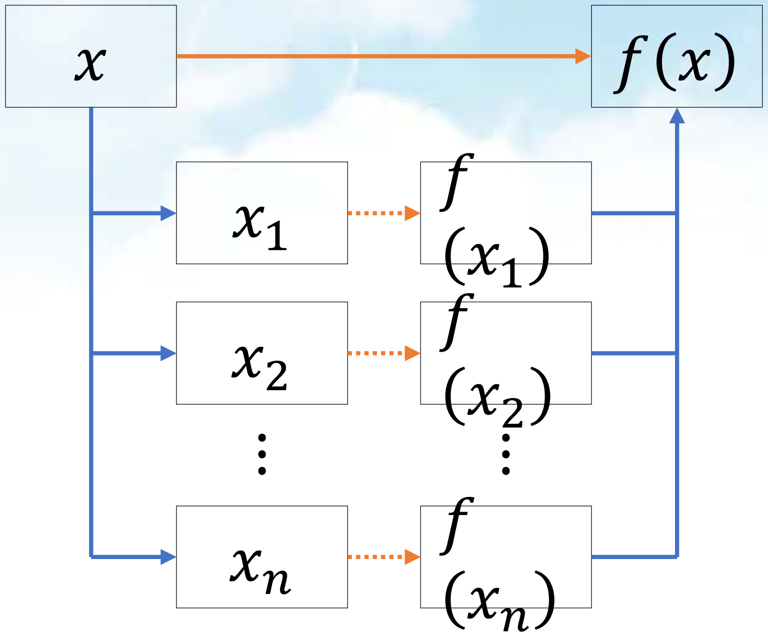
Contribution

2. As an application, we propose CSIDH-based (post-quantum) AKE with optimal tightness, following the construction of Cohn-Gordon *et al.* [CCG+18]
   - Cohn-Gordon *et al.*'s AKE is based on DH, thus not quantum-resistant.
   - It is the fastest CSIDH-based AKE when we aim at 110-bits security level.

[CCG+18] K. Cohn-Gordon, C. Cremers, K. Gjøsteen, H. Jacobsen, and T. Jager. Highly Efficient Key Exchange Protocols with Optimal Tightness. In CRYPTO 2019

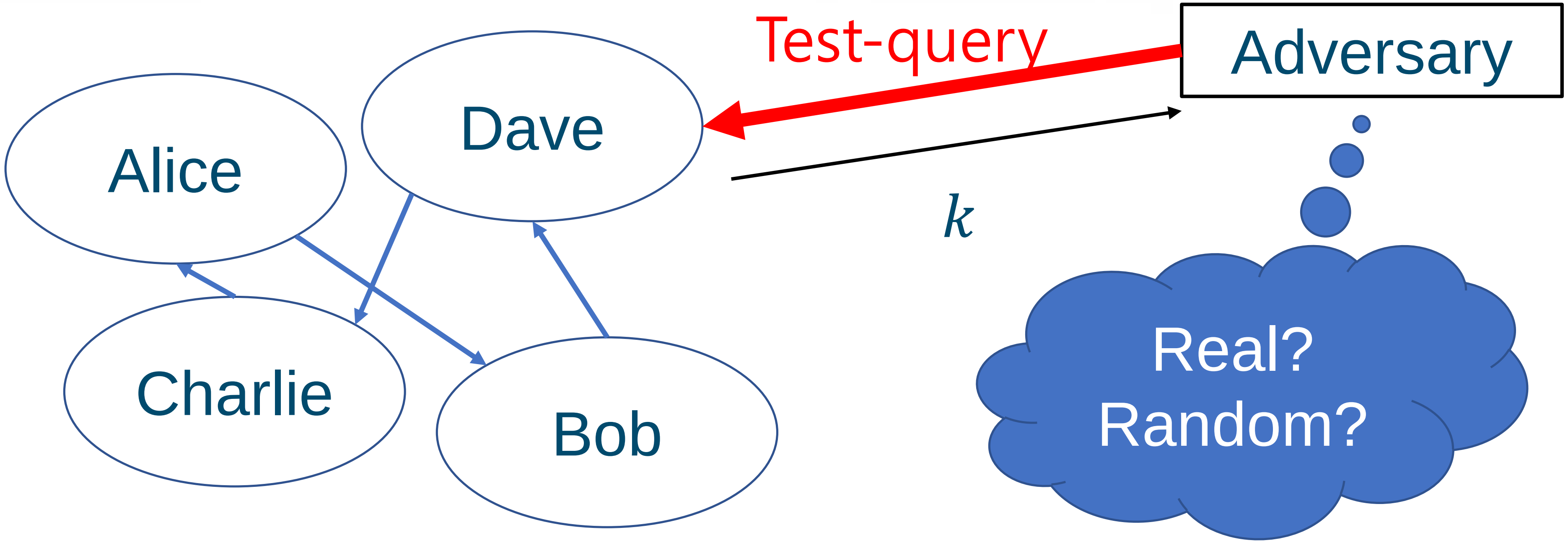
Random Self-Reducibility (RSR)

- Let P be a problem to evaluate $f(x)$ given uniformly chosen x.
- P is random self-reducible when we can generate multiple instances $x_1, \ldots, x_n$ s.t.
  - If any one of $f(x_i)$ is given, we can compute $f(x)$ efficiently, and
  - $x_1, \ldots, x_n$ are independent and uniform.
- RSR is useful to achieve tightness



AKE's security model

- We assume multiple users
- Adversary chooses users to get real-or-random keys (RoR)
  - To decide real-or-random is hard ⇒ AKE is secure



RSR and tight AKE

- Embedding the instance to multiple users lowers the security loss, but
  - we should compute $f(x)$ when any embedded user is tested, and
  - public keys of the embedded users must be independent.
- These two requirements are similar to the definition of RSR

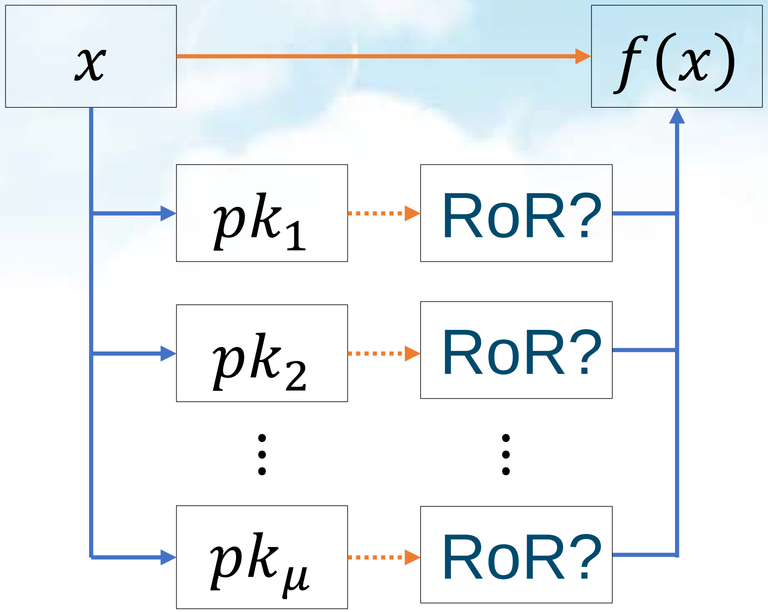


Table of Contents

Hard Problems for Diffie-Hellman

- Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of prime order p.

- Computational Diffie-Hellman Problem (CDH problem)
  - Given $X = g^x, Y = g^y$, compute $Z = g^{xy}$.

- Decisional Diffie-Hellman Problem (DDH problem)
  - Given $X = g^x, Y = g^y, Z \in \mathbb{G}$, decide $Z = g^{xy}$ or not.

- DDH and CDH are RSR.

RSR of CDH

- Given CDH-instance $X = g^x, Y = g^y$, rerandomize as

$$X_i = X^{a_i}, Y_i = Y^{b_i} \ \left(a_i, b_i \leftarrow \mathbb{Z}_p\right)$$

- If i-th answer $Z_i = g^{a_i b_i xy}$ is given, we can recover g^{xy} by computing $Z_i^{(a_i b_i)^{-1}}$.
- Independency follows from that of a_i, b_i.

RSR of DDH (1/2)

- DDH instance: $(X, Y, Z) = (g^x, g^y, g^z)$
- 1st idea: $X_i = X^{a_i}, Y_i = Y^{b_i}$
  - $Z = g^{xy} \Rightarrow Z_i = g^{a_i x b_i y} = Z^{a_i b_i}$, so $Z_i = Z^{a_i b_i}$?
  - When $Z \neq g^{xy}$, Z_i must be independent to X_i and Y_i, but $Z^{a_i b_i}$ is not independent of X_i and Y_i for fixed X, Y, and Z.
  - This idea does not to work.

RSR of DDH (2/2)

- DDH instance: $(X, Y, Z) = (g^x, g^y, g^z)$
- 2nd idea: $X_i = X^{a_i} \cdot g^{c_i} = g^{a_i x + c_i}, Y_i = Y \cdot g^{b_i}$
  - $Z = g^{xy} \Rightarrow Z_i = g^{(a_i x + c_i)(y + b_i)} = Z^{a_i} \cdot X^{a_i b_i} \cdot Y^{c_i} \cdot g^{b_i c_i}$, so $Z_i = Z^{a_i} \cdot X^{a_i b_i} \cdot Y^{c_i} \cdot g^{b_i c_i}$?
  - In this case, when $Z \neq g^{xy}$, Z_i is independent of X_i and Y_i.
- Two operations (exponentiation & multiplication) are used in DDH-case
  - In CDH-case, we use only exponentiation.

Table of Contents

Hard Homogeneous Spaces [Cou06]

- $\mathbb{G}$: abelian group, H: finite set
- A group action $\star: (g \in \mathbb{G}, h \in H) \mapsto g \star h \in H$ is a map such that
  - $^\forall g_1, g_2 \in \mathbb{G}, g_1 \star (g_2 \star h) = (g_1 g_2) \star h$, and
  - For the unit element $e \in \mathbb{G}$, $^\forall h \in H, e \star h = h$.
- $\star$ is simply transitive if a map $g \mapsto g \star h$ is bijective for all $h \in H$.
- If there is an action which is simply transitive and hard to invert, $(\mathbb{G}, H)$ is called Hard Homogeneous Space (HHS).

[Cou06] Jean-Marc Couveignes. Hard Homogeneous Spaces. Cryptology ePrint Archive, Report 2006/291, 2006

HHS-based Key Exchange

- We can construct a DH-like key exchange with HHS.

Public parameter: $x_0 \in H$

Alice		Bob
$a \leftarrow \mathbb{G}$, $A = a \star x_0$	A → ← B	$b \leftarrow \mathbb{G}$, $B = b \star x_0$
$K_A = a \star B$		$K_B = b \star A$

- We can realize HHS with elliptic curves and isogenies, and CSIDH is a key exchange protocol of this type.

Hard Problems for CSIDH (HHS)

- CSI-CDH problem
  - Given $a \star x_0, b \star x_0$, compute $ab \star x_0$.
- CSI-DDH problem
  - Given $a \star x_0, b \star x_0$ and $C \in H$, decide whether $C = ab \star x_0$ or not.
- These problems are considered to be hard even for quantum computers, so CSIDH is regarded to be post-quantum key exchange.

Contribution: RSR of CSI-CDH Problem

- We can prove that CSI-CDH problem is RSR.
- Given $A = a \star x_0, B = b \star x_0$, we rerandomize as
$$A_i = \rho_i \star A, B_i = \eta_i \star B.$$
- i-th answer is $C_i = \rho_i \eta_i ab \star x_0$, so $(\rho_i \eta_i)^{-1} \star C_i = ab \star x_0$.
- Since the map $g \mapsto g \star A$ is bijective, A_i, B_i are independent and uniform.
- In computational case, CDH-technique can be used.

CSI-DDH seems not to be RSR

- In DDH-case, we rerandomized like $X^{a_i} \cdot g^{c_i}$ for independency.
  - In CSIDH-case, X^{a_i} and g^{c_i} are elements in H, finite set, so we have no operation between them.
  - In CSIDH, we cannot use the same technique as in DDH-case.
- This "lack of operation" is inevitable for quantum-resistance.
  - If we can use the same technique in HHS, then we can invert the action with Shor's algorithm.

We achieve quantum-resistance
at the expense of utility.

Table of Contents

Comparison for 110-bit security level

Protocol	Security loss	Underlying Problems	Parameters [CLM+18]
CSIDH UM [FTY19]	$\mu^2 l^2$	2DDH	CSIDH-1024
CSIDH Biclique [FTY19]	$(\max(\mu, l))^2$	2GDH	CSIDH-512
Proposed protocol	μ	CSI-stDH	CSIDH-512

- $\mu = 2^{16}$ users and at most $l = 2^{16}$ sessions per user.
- We assume that the best way to solve these problems is to invert the group action

[CLM+18] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. CSIDH: An Effic -ient Post-Quantum Commutative Group Action. In *ASIACRYPT 2018*

[FTY19] Atsushi Fujioka, Katsuyuki Takashima, and Kazuki Yoneyama. One-Round Auth enticated Group Key Exchange from Isogenies. *In ProvSec 2019*

Comparison for 110-bit security level

Protocol	Parameters	# of actions	Expected clock time [BDLS20]
CSIDH UM [FTY19]	CSIDH-1024	3	$719M \times 3 = 2{,}157M$
CSIDH Biclique [FTY19]	CSIDH-512	5	$120M \times 5 = 600M$
Proposed protocol	CSIDH-512	4	$120M \times 4 = 480M$

- We take $\mu = 2^{16}, l = 2^{16}$ here.
- Our protocol is the fastest CSIDH-based AKEs.

[FTY19] Atsushi Fujioka, Katsuyuki Takashima, and Kazuki Yoneyama. One-Round Authenticated Group Key Exchange from Isogenies. *In ProvSec 2019*

[BDLS20] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith, Faster computation of isogenies of large prime degree. Cryptology ePr-int Archive, Report 2020/341

Table of Contents

Conclusion & Future works

Conclusion:

- We showed that the computational problem and the gap problem of CSIDH are RSR.
- As an application, we proposed an optimally-tight post-quantum AKE.

Future works:

- To prove RSR of CSI-DDH problem in another way
- To propose an optimally-tight post-quantum AKE in stronger models.

Thank you for listening!